SVKM's

D. J. Sanghvi College of Engineering

Program: B.Tech in Information Technology **Academic Year: 2022** **Duration: 3 hours**

Date: 05.01.2023

Time: 10:30 am to 01:30 pm

Subject: Cryptography and Network Security (Semester V) **Marks: 75**

Q1 (a)	How is security achieved in Transport and Tunnel modes of IPSEC? Explain role of AH and ESP **OR** User wishes to do online transaction on Amazon.com. Identify and explain which protocol they will use to establish secure communication channel and mutual authentication of client and server.	[10] [10]
Q1 (b)	Encrypt the message "The house is being sold tonight" using Vigenere Cipher with key = "lemon". Ignore the spaces between the words. Decrypt the message to get the original plaintext. OR Use the Playfair cipher with the keyword "HEALTH" to encipher the message "Life is full of Surprises"	[05] [05]
Q2 (a)	Describe in detail the key generation in AES algorithm and its expression format **OR** What are the various modes of operations OF BLOCK CIPHORS. Explain any 2 in detail.	[08] [08]
Q2 (b)	Draw the general structure of DES and explain the encryption process.	[07]
Q3 (a)	If A and B wish to use RSA to communicate securely A chooses public key (e, n) as (7,247) and B chooses public key (e, n) as (5,221). 1. Calculate A's Private key 2. Calculate B's Private key 3. What will be the cipher text sent by A to B if A wishes to send M=5 securely to B	[08]
Q3 (b)	Given the super increasing tuple b= (2, 3, 7, 14, 30, 57, 120, 251), random integer r=41 and modulus n=491. Encrypt M=150 using knapsack cryptosystem. **OR** Using Rabin cryptosystem with p=47 and q=11, encrypt ~~p~~ P=17 to find the ciphertext. Use Chinese remainder theorem to find four possible plain text.	[07] [07]
Q4 (a)	Explain the process of deriving eighty 64-bitwords from 1024 bits for processing of a single blocks and also discuss single round function in SHA-512 algorithm. Show the values of W16, W17, W18 and W19. **OR** The cipher text obtained by using double transposition cipher is TIYTEAOZHMCSEANGYKTN. If the permutation key used for encryption is 31452, decrypt the above cipher text.	[10] [10]
Q4 (b)	Differentiate between MAC and MDC	[05]

Q5 (a)	Explain man in the middle attack on Diffie Hellman. Discuss the solution for the same **OR** How authentication is achieved in Kerberos. Explain authentication with respect to the exchange of key between Client and Server	[10] [10]
Q5 (b)	Susan wants to send a secret document to Bob using asymmetric Cryptosystem. How Digital Certificates can help her in doing the same. Explain the format of X.509 certificate	[05]